

# Re: Windows 2003 server Network Security

---

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-12/msg00467.html>

---

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Fri, 23 Dec 2005 16:50:37 -0600
- 

If you are using managed switches they may have the capability to manage port access by mac address either from a table of mac addresses that can be manually configured and from putting the switch in learning mode when you are sure only authorized devices are connected to the network and many switches can do 802.1X which requires the computer be authenticated before the switch port allows access though it also requires compatible operating systems and a Certificate Authority. Currently there is not way to use Group Policy to configure "wired" 802.1X like there is for wireless 802.1X.

Another possibility is to implement ipsec in your domain that can be managed via Group Policy. Computers that have an ipsec require policy will not communicate with computers that do not have a compatible authentication method and in a domain by default Kerberos would be used for computer authentication that would rule out non domain computers. Ipsec is a somewhat complex topic and special considerations must be made for domain controllers since they are the KDC but the link below on ipsec domain isolation is a great start. Possibly something like ISA 2004 as your firewall and using ipsec could be used to prevent users on non domain computers from accessing the internet since the computer would need to access the ISA 2004 server to authenticate the domain user. Otherwise it is very difficult to stop users from accessing the internet if all they need is access to the default gateway that can found out rather easily and a user could use static IP configuration to bypass restrictions placed on a DHCP scope. --- Steve

<http://www.microsoft.com/technet/security/topics/architectureanddesign/ipsec/ipsecch1.msp>  
<http://support.microsoft.com/?kbid=254949> --- important info on domain ipsec.

"Larry Bird" <LarryBird@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:AA0A4EB4-869F-4E84-8D61-2EBB09D1A19A@xxxxxxxxxxxxxxxxxxxx>  
>I want to lock down my network from PCs for Laptops outside the company.  
> Basically I do not want anyone to be able to plug in his or her laptop  
> computer via an RJ45 connection and have any access to resources without  
> signing in with a valid userid and password. I don't want them to have a  
> DHCP IP address to surf the Internet unless authorized via their userid  
> and  
> password.  
>  
> Where do I start to implement these restrictions?

Re: Windows 2003 server Network Security

>  
> Thanks  
>  
>

.

- 
- Prev by Date: [\*Re: Windows 2003 server Network Security\*](#)
  - Next by Date: [\*SSPI client to ldap Server – Error at last stage of n-way authentication check\*](#)
  - Previous by thread: [\*Re: Windows 2003 server Network Security\*](#)
  - Next by thread: [\*SSPI client to ldap Server – Error at last stage of n-way authentication check\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)